Title: Methods For Computing The CRC Of A Message From
The Incremental CRCs Of Composite Sub-Messages
Inventors: Vicente V. Cavanna; Patricia A. Thaler
Atty. Docket No.: 10011175
Atty.: Pamela Lau Kee Tel.: (408) 553-3059

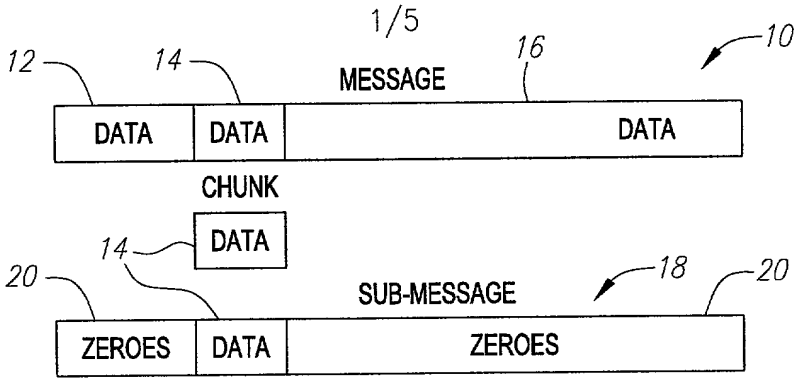

FIG. 1

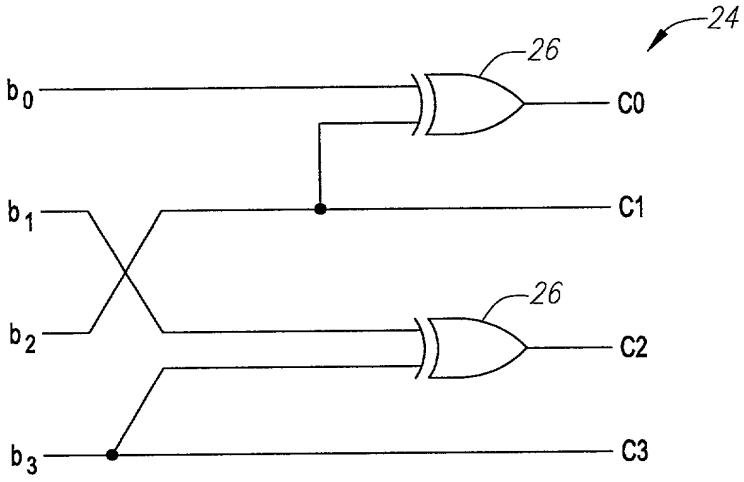

FIG. 2

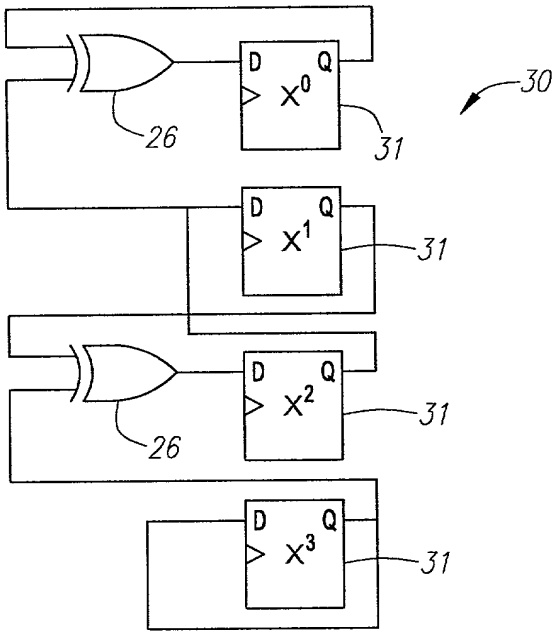

FIG. 3

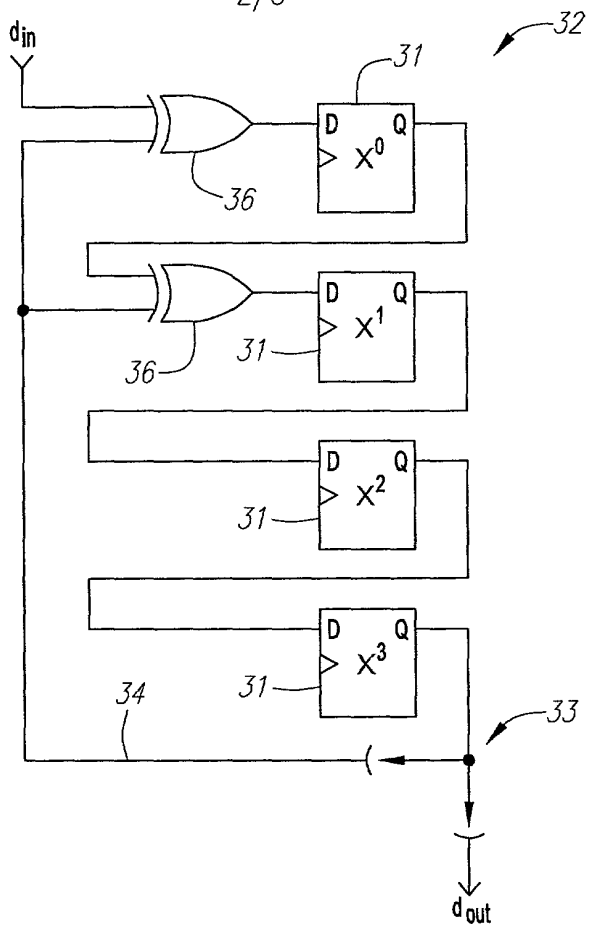

FIG. 4

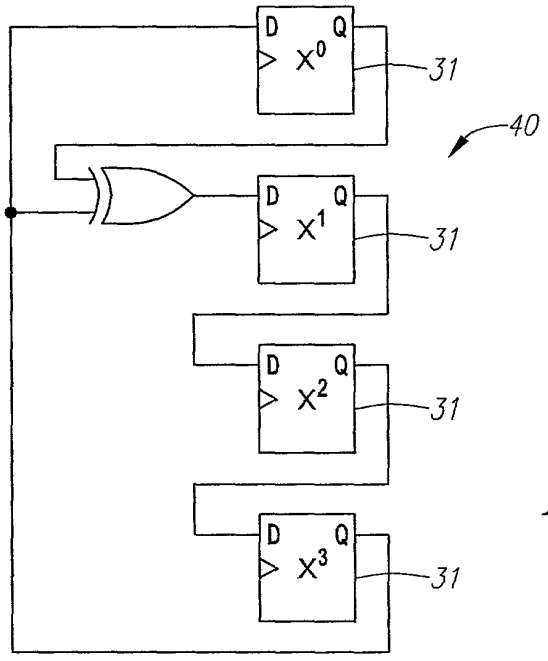

FIG. 5

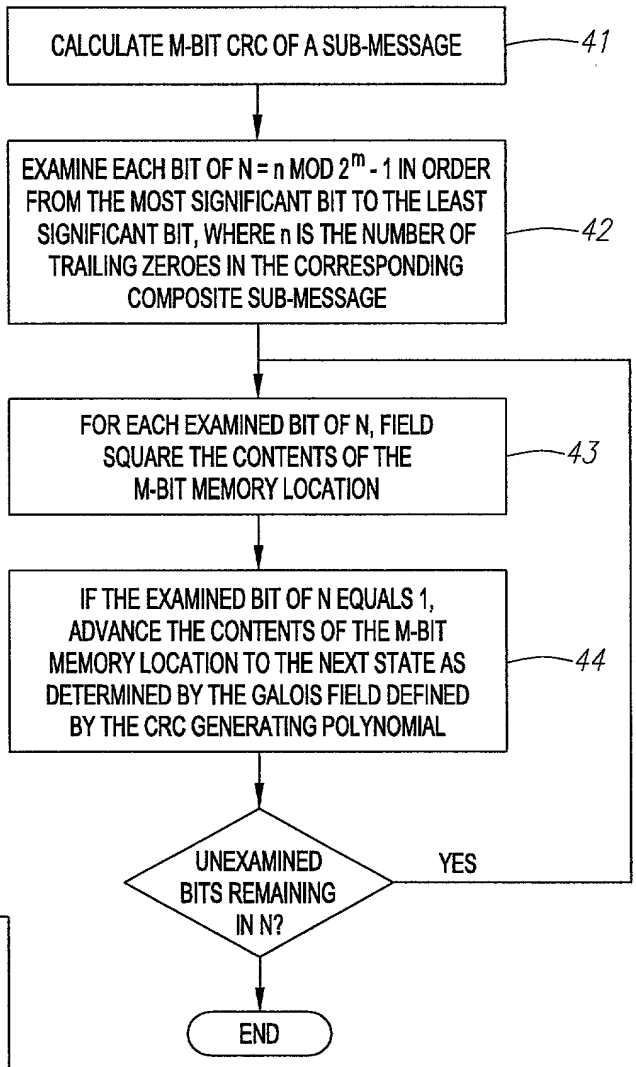
CALCULATE M-BIT CRC OF A SUB-MESSAGE
41
EXAMINE EACH BIT OF N = n MOD 2^m - 1 IN ORDER FROM THE MOST SIGNIFICANT BIT TO THE LEAST SIGNIFICANT BIT, WHERE n IS THE NUMBER OF TRAILING ZEROES IN THE CORRESPONDING COMPOSITE SUB-MESSAGE
42
FOR EACH EXAMINED BIT OF N, FIELD SQUARE THE CONTENTS OF THE M-BIT MEMORY LOCATION
43
IF THE EXAMINED BIT OF N EQUALS 1, ADVANCE THE CONTENTS OF THE M-BIT MEMORY LOCATION TO THE NEXT STATE AS DETERMINED BY THE GALOIS FIELD DEFINED BY THE CRC GENERATING POLYNOMIAL
44
UNEXAMINED BITS REMAINING IN N?
YES
END

FIG. 6

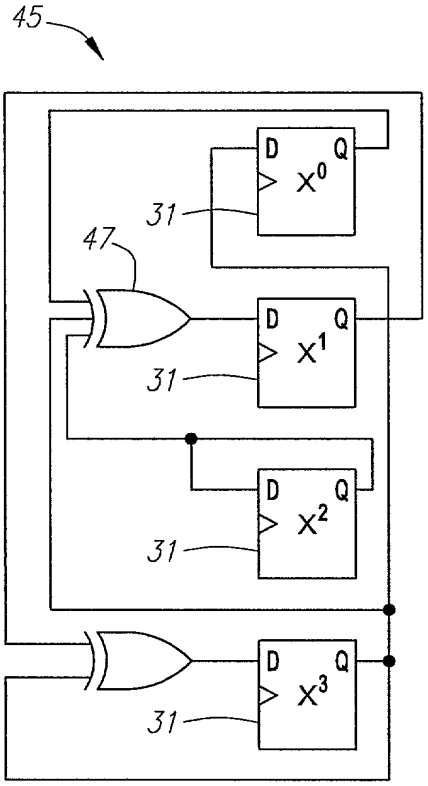
45
D
Q
X^0
31
47
X^1
X^2
X^3

FIG. 7

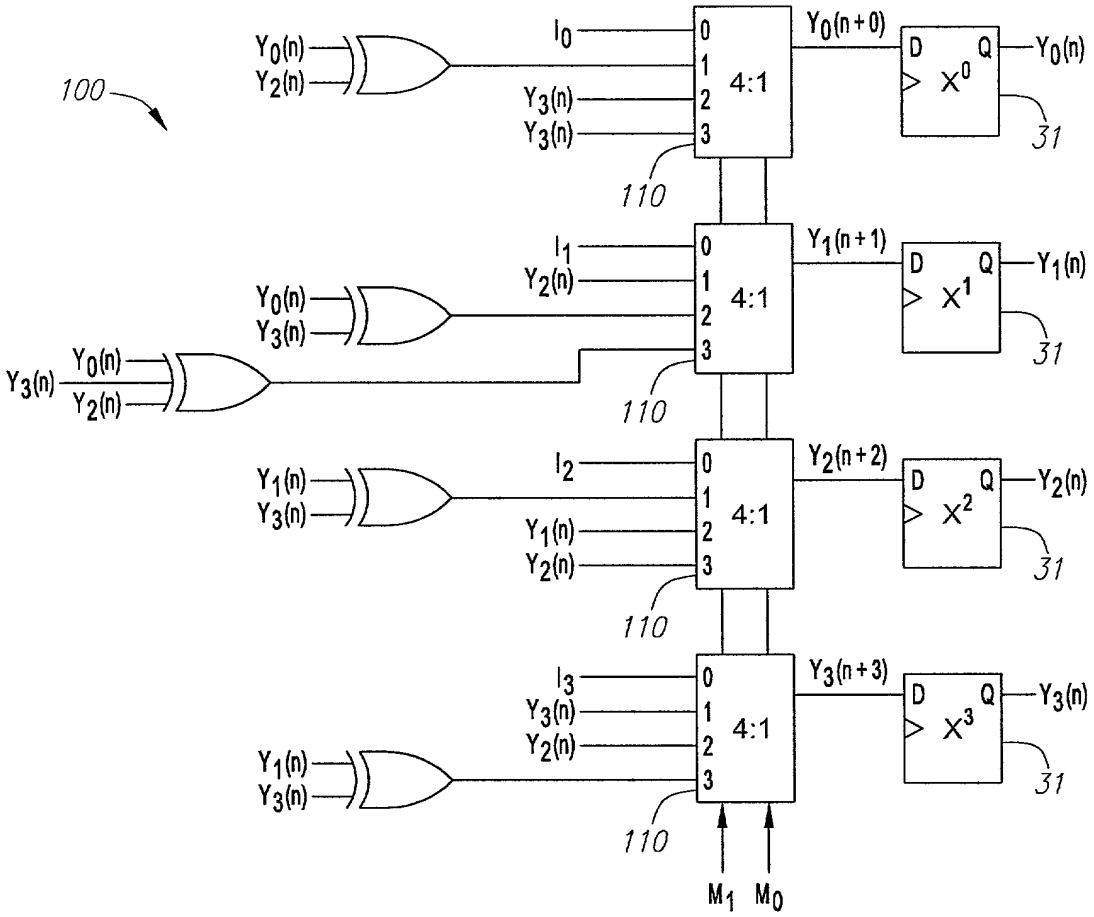
100
$Y_0(n)$
$Y_2(n)$
I_0
$Y_3(n)$
$Y_3(n)$
4:1
$Y_0(n+0)$
D
Q
X^0
$Y_0(n)$
31
110
I_1
$Y_2(n)$
$Y_0(n)$
$Y_3(n)$
$Y_3(n)$
$Y_0(n)$
$Y_2(n)$
4:1
$Y_1(n+1)$
X^1
$Y_1(n)$
I_2
$Y_1(n)$
$Y_3(n)$
$Y_1(n)$
$Y_2(n)$
4:1
$Y_2(n+2)$
X^2
$Y_2(n)$
I_3
$Y_3(n)$
$Y_2(n)$
$Y_1(n)$
$Y_3(n)$
4:1
$Y_3(n+3)$
X^3
$Y_3(n)$
M_1
M_0

FIG. 8

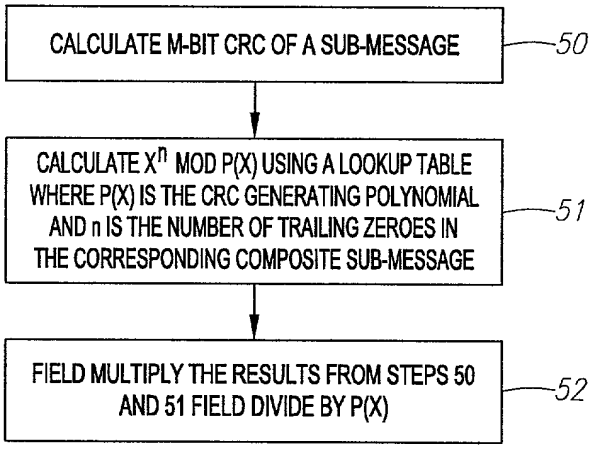
CALCULATE M-BIT CRC OF A SUB-MESSAGE
50
CALCULATE X^n MOD P(X) USING A LOOKUP TABLE WHERE P(X) IS THE CRC GENERATING POLYNOMIAL AND n IS THE NUMBER OF TRAILING ZEROES IN THE CORRESPONDING COMPOSITE SUB-MESSAGE
51
FIELD MULTIPLY THE RESULTS FROM STEPS 50 AND 51 FIELD DIVIDE BY P(X)
52

FIG. 9a

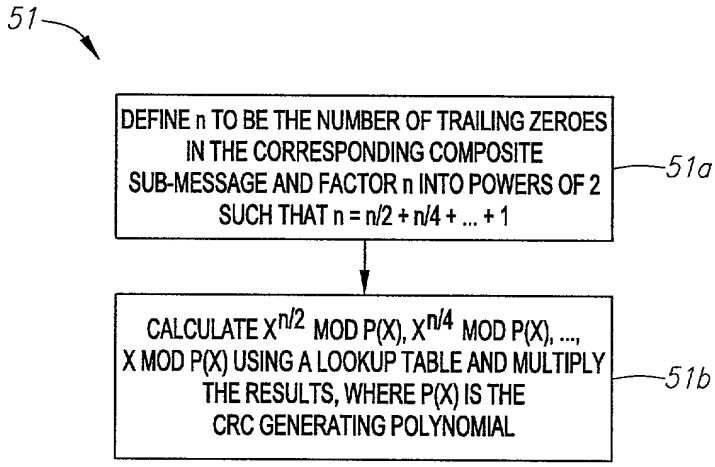
51
DEFINE n TO BE THE NUMBER OF TRAILING ZEROES IN THE CORRESPONDING COMPOSITE SUB-MESSAGE AND FACTOR n INTO POWERS OF 2 SUCH THAT n = n/2 + n/4 + ... + 1
51a
CALCULATE $X^{n/2}$ MOD P(X), $X^{n/4}$ MOD P(X), ..., X MOD P(X) USING A LOOKUP TABLE AND MULTIPLY THE RESULTS, WHERE P(X) IS THE CRC GENERATING POLYNOMIAL
51b

FIG. 9b